UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/828,443	04/20/2004	Richard Baer	10030568-1	4008

7590 03/26/2008

AGILENT TECHNOLOGIES, INC.
Legal Department, DL 429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599

EXAMINER	
KOZIOL, STEPHEN R	
ART UNIT	PAPER NUMBER
2624	

MAIL DATE	DELIVERY MODE
03/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/828,443	BAER, RICHARD	
	Examiner	Art Unit	
	STEPHEN R. KOZIOL	2624	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14,17-28,30,32 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14,17-28,30,32 and 33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the appeal brief filed on 12/18/2007 PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Samir A. Ahmed/

Supervisory Patent Examiner, Art Unit 2624.

2. Claims 1-14, 17-28, 30, 32 and 33 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims (1-3, 10, and 26-27) are rejected under 35 U.S.C. 102(b) as being anticipated by Doyle et al. U.S. Pre-Grant Publication 2002/0095587 A1, hereinafter Doyle.

Regarding claim 1, Doyle discloses a biometric data card *(see Fig. 5 item 510 & pars. 0035-36)* comprising:

i. an image sensor for capturing an image of a biometric feature of a user of the biometric data card and producing first image data representing the image (*see Fig. 5 item 520 & pars. 0035-36 and 0080, where the image sensor located on the biometric data card gathers, e.g., a fingerprint representing first image data of a user)*;

ii. a memory operable to store second image data (*see Fig. 5 item 514 as described in pars. 0035-36 and 0080 where the memory stores template images of authorized users*); and

iii. a processor in communication with said image sensor and said memory, said processor operable to perform a comparison of the first image data with the second image data, and, to generate, in response to the comparison, authentication information representative of an authentication of the user (*see Fig. 5 item 512 as described in pars.*

0035-36 and 0080 where the processor compares the first image data gathered by the card sensor with the stored images of authorized users in order to generate an authentication signal);

iv. wherein the processor is configured for transmitting the authentication information through a card interface in a terminal so as to authenticate the user to the terminal separate from said image sensor, said memory, and said processor *(Fig. 6 as described in par. 0081 where the I/O bus is the interface through which authentication is transferred between the smart card and the terminal).*

Regarding claim 2 Doyle teaches the biometric data card of claim 1, further comprising: an interface operable to transmit the authentication information from the biometric data card to a terminal *(Fig. 6 as described in par. 0081 where the I/O bus is the interface through which authentication is transferred between the smart card and the terminal).*

Regarding claim 3 Doyle teaches the biometric data card of claim 2 wherein said interface comprises a contact pad operable to form an electrical connection to the terminal, said contact pad being further operable to transmit the authentication information from the biometric data card to the terminal via the electrical connection *(See par. 0062 for the electrical contact pad).*

Regarding claim 10 Doyle teaches the biometric data card of claim 1 wherein the biometric feature is at least one of an iris of an eye of the user, a facial feature of the user or a fingerprint of a finger of the user *(see par. 0080, where, e.g., a fingerprint is used as the biometric feature).*

Regarding claim 26 Doyle discloses a method for authenticating a user using a biometric data card, the method comprising:

i. capturing an image of a biometric feature of a user on an image sensor in the biometric data card (*see Fig. 5 item 520 & pars. 0035-36 and 0080, where the image sensor located on the biometric data card gathers, e.g., a fingerprint representing first image data of a user)*;

ii. producing in the biometric data card first biometric image data in response to ~~an~~ the image of a biometric feature of the user captured by said image sensor (*see Fig. 5 item 520 & pars. 0035-36 and 0080, where the image sensor located on the biometric data card gathers, e.g., a fingerprint representing first image data of a user)*;

iii. comparing in said biometric data card the first biometric image data with second biometric image data (*see Fig. 5 item 514 as described in pars. 0035-36 and 0080 where the memory stores template images of authorized users*); and

iv. authenticating the user in response to said comparing *(see Fig. 5 item 512 as described in pars. 0035-36 and 0080 where the processor compares the first image data gathered by the card sensor with the stored images of authorized users in order to generate an authentication signal).*

Regarding claim 27 Doyle teaches the method of claim 26, further comprising: transmitting an authentication signal from the biometric data card to a terminal *(Fig. 6 as described in par. 0081 where the I/O bus is the interface through which authentication is transferred between the smart card and the terminal)*; and in response to the authentication

signal, allowing the terminal to interact with the user *(see pars. 0083-84, where, e.g., an ATM embodiment is disclosed).*

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.
>
> The factual inquiries set forth in **Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966)**, that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows: ***(See MPEP Ch. 2141)***
>
> a. Determining the scope and contents of the prior art;
> b. Ascertaining the differences between the prior art and the claims in issue;
> c. Resolving the level of ordinary skill in the pertinent art; and
> d. Evaluating evidence of secondary considerations for indicating obviousness or nonobviousness.

6. Claims (4, 6-7, 28, 30) are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. U.S. Pre-Grant Publication 2002/0095587 A1 in view of Campisi et al. U.S. Pre-Grant Publication 2007/0220272 A1, hereinafter Campisi.

Regarding claims 4 and 28, Doyle teaches the biometric data card of claim 2 and system of claim 28, but is silent on the processor further operable to determine adjustment information for the terminal to use in capturing an additional image of the biometric feature and to transmit the adjustment information to the terminal via the interface. However, Campisi cures the aforementioned deficiencies of Doyle by teaching a comparable smart card with an image sensor, wherein the card may prompt the user for a redo scan if, e.g., the processor in the card determines the fingerprint was not acceptably recorded *(see Campisi par. 0046).* Therefore, a person having ordinary skill in the image processing arts at the time of the invention would have

found it obvious to improve upon the smart card of Doyle by incorporating the "redo scan" functionality of Campisi to yield the predictable beneficial result of requesting additional adjustment information when the processor determines an additional image needs to be captured.

Regarding claim 6, Campisi further teaches the biometric data card of claim 1, wherein said processor is further operable to extract first feature characteristics from the first image data and second feature characteristics from the second image data, and to compare the first feature characteristics to the second feature characteristics to determine the authentication information *(see Campisi Fig. 10 as described in par. 0043 wherein the comparison between the stored fingerprint and the presently scanned fingerprint utilizes minutia obtained from the images).*

Regarding claim 7, Campisi further teaches the biometric data card of claim 1, wherein said second image data comprises second feature characteristics; and said processor is further operable to extract first feature characteristics from the first image data and to compare the first feature characteristics to the second feature characteristics to determine the authentication information *(see Campisi Fig. 10 as described in par. 0043 wherein the comparison between the stored fingerprint and the presently scanned fingerprint utilizes minutia obtained from the images).*

Regarding claim 30, Campisi discloses the method of claim 26 wherein:
Said producing includes extracting first feature characteristics from the image data to produce the first biometric image data; the second biometric image data includes second feature characteristics extracted from a previous image; and said comparing includes comparing the first feature characteristics to the second feature characteristics *(see Campisi Fig. 10 as described in*

par. 0043 wherein the comparison between the stored fingerprint and the presently scanned fingerprint utilizes minutia obtained from the images).

7. Claims (5, 11-13, 17-24 and 32) are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. U.S. Pre-Grant Publication 2002/0095587 A1 in view of Angelo US 6,182,892 B1, hereinafter Angelo.

Regarding claim 5 Doyle teaches the biometric data card of claim 1, further comprising: an element for transferring the image to said image sensor *(Doyle Fig. 6 as described in par. 0081).* However, Doyle's transfer element is an electrical transfer element, not an optical element as required by claim 5. Angelo teaches a comparable biometric authentication smart card wherein the optical transfer between the card and a terminal is disclosed *(see Angelo col. 5 lines 35-40, where an optical transfer element is disclosed).* To arrive at instant Claim 5, one need only to substitute the Doyle's electrical transfer element for Angelo's optical transfer element, which, as evidenced by Angelo, would have been reasonable to one skilled in the art. Therefore, it would have been obvious to a person having ordinary skill in the image processing arts at the time of the invention to substitute Doyle's electrical transfer element for Angelo's optical transfer element to achieve the predictable result of transferring an image to an image sensor.

Regarding claim 11, Angelo discloses a terminal for authenticating a user of the terminal comprising:

i. an optical interface configured to receive light reflected from a biometric feature of the user *(see Angelo, Fig. 8 as described in col. 9 lines 46-56);*

ii. an optical element optically coupled to said optical interface via an optical path, said optical element operable to form an image of the biometric feature from the reflected light and to direct the image onto an image sensor *(see Angelo, Fig. 6 as described in col. 9 line 57 thru col. 10 line 20);* and

iii. a card interface configured to receive a biometric data card and operable to authenticate the user based on the image and to provide an authentication signal to the terminal and said card interface being optically coupled to said optical interface and said optical element to direct the image onto the image sensor *(see Angelo, Fig. 8 and as described in col. 9 lines 46-56, where the optical card interface and authentication is disclosed).*

Angelo fails to disclose that the image sensor is located on the biometric data card, as required by instant claim 11. (In each of Angelo's embodiments the image sensor is part of the terminal.) However, Doyle cures the aforementioned deficiencies of Anglo by teaching a comparable biometric smart card having an image sensor located on the smart card *(see Doyle pars. 0035-36 and 0080).* It would have been obvious to a person having ordinary skill in the image processing arts at the time of the invention to modify Angelo's smart card to include Doyle's image sensor to achieve the added layer of security that comes with sensing the biometric feature of a user directly on the smart card.

Regarding claim 12 Doyle further teaches the terminal of claim 11, wherein said card interface is operable to receive the authentication signal *(Doyle Fig. 6 as described in par. 0081 where the I/O bus is the interface through which authentication is transferred between the smart card and the terminal).*

Regarding claim 13 Doyle further teaches the terminal of claim 12, wherein said card interface *(See par. 0062 for the electrical contact pad).*

Regarding claim 17 Angelo further teaches the terminal of claim 11 further comprising: a processor connected to receive the authentication signal and operable in response to the authentication signal to allow the terminal to interact with the user *(see Angelo Fig. 8—Host CPU as explained in col. 9 lines 46-56).*

Regarding claim 18 Angelo further teaches the terminal of claim 11 further comprising a user interface *(see Angelo Fig. 6 item 110, which is an interface through which the user interacts with the terminal, as described in col. 9 line 57 thru col. 10 line 20).*

Regarding claim 19 Angelo further teaches the terminal of claim 11 further comprising: an illumination source disposed in relation to said optical interface to illuminate the biometric feature of the user *(see Angelo Fig. 6 item 120 (laser diode) as described in col. 9 line 57 thru col. 10 line 20).*

Regarding claim 20 Angelo further teaches the terminal of claim 11 wherein said optical element includes a lens *(see Angelo Fig. 6 item 128 (laser diode) as described in col. 9 line 57 thru col. 10 line 20 as well as col. 5 lines 35-54).*

Regarding claim 21 Angelo further teaches the terminal of claim 11 further comprising: transfer optics located between said optical interface and said optical element to direct the reflected light to said optical element *(see Angelo Fig. 6 item 112 "light pipe" as described in col. 9 line 57 thru col. 10 line 20 as well as col. 12 lines 5-9).*

Regarding claim 22 Angelo further teaches the terminal of claim 11 wherein the terminal is part of a cellular telephone, pay phone, credit card machine or identification terminal *(see Angelo col. 11 lines 54-59 as well as Fig. 8 as described in col. 9 lines 46-56).*

Regarding claim 23 Doyle discloses a system for authenticating a user, comprising: a biometric data card including an image sensor for capturing an image of a biometric feature of the user and for producing first image data representing the image, said biometric data card operable to perform a comparison of the first image data with second image data, and, to generate, in response to the comparison, authentication information representative of an authentication of the user (*see Doyle Fig. 5 item 512 as described in pars. 0035-36 and 0080 where the processor compares the first image data gathered by the card sensor with the stored images of authorized users in order to generate an authentication signal).*

Angelo further discloses a terminal including a card interface configured to receive said biometric data card and operable to receive the authentication information from said biometric data card, said terminal further including an optical element arranged to direct light from the biometric feature onto the image sensor *(see Angelo, Fig. 6 as described in col. 9 line 57 thru col. 10 line 20 as well as, Fig. 8 as described in col. 9 lines 46-56, where the optical card interface, image sensor and authentication is disclosed).*

Regarding claim 24, Angelo further discloses the system of claim 23, wherein said card interface includes a first contact pad operable to form an electrical connection to a second contact pad on the biometric data card, the authentication signal being transmitted from said biometric data card to said terminal via the electrical connection *(see Angelo Fig. 6 items 116*

and 118, the chip card reader as described in col. 7 lines 9-13, which is common to each of Angelo's disclosed embodiments).

Regarding claim 32 Angelo further discloses the method of claim 26 wherein said producing further includes illuminating the biometric feature (*see Angelo Fig. 6 item 120 (laser diode) as described in col. 9 line 57 thru col. 10 line 20).*

8. Claims (14 and 25) are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. U.S. Pre-Grant Publication 2002/0095587 A1 in view of Angelo US 6,182,892 B1 further in view of Campisi et al. U.S. Pre-Grant Publication 2007/0220272 A1.

Regarding claims 14 and 25, Angelo in view of Doyle teach the terminal of claim 12 and system of claim 25 as indicated above, but neither Doyle nor Angelo further teach the terminal wherein the card interface is further operable to receive a feedback signal from the biometric data card, the feedback signal providing adjustment information to the terminal for use in capturing an additional image of the biometric feature. However, Campisi cures the aforementioned deficiencies of Angelo in view of Doyle by teaching a comparable smart card with an image sensor, wherein the card may prompt the user for a redo scan if, e.g., the processor in the card determines the fingerprint was not acceptably recorded *(see Campisi par. 0046).* Therefore, a person having ordinary skill in the image processing arts at the time of the invention would have found it obvious to improve upon the smart card of Angelo in view of Doyle by incorporating the “redo scan" functionality of Campisi to yield the predictable beneficial result of requesting additional adjustment information when the processor determines an additional image needs to be captured.

9. Claims (8-9 and 33) are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. U.S. Pre-Grant Publication 2002/0095587 A1 in view of Janiak et al. U.S. Pre-Grant Publication 2002/0030581 A1, hereinafter Janiak.

Regarding claims 8 and 9, Doyle does not explicitly state that the image sensor in the biometric data card of claim 1 is a CMOS and CCD image sensor, as required by instant claims 8 and 9. However, Janiak discloses a comparable smart card authentication system that utilizes either a CCD or CMOS image sensor *(see Janiak par. 0035)*. The salient difference between Janiak and Doyle is the location of the image sensor: Doyle discloses an embodiment wherein the image sensor is located directly on the smart card *(see Claim 1 supra)* while Janiak discloses the CCD or CMOS image sensor on the terminal, as opposed to the smart card *(see Janiak par. 0035)*. It would have been obvious to a person having ordinary skill in the image processing arts at the time of the invention to use the well-known (as evidenced by Janiak) CCD and CMOS image sensors as the image sensor located directly on Doyle's disclosed smart card to achieve the predictable result of capturing a biometric feature of the user.

Regarding claim 33 Janiak further discloses the method of claim 26 further comprising communicating with a remoter server based on said authenticating *(see Janiak par. 0043 and Fig. 13)*

Contact

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steve Koziol whose telephone number is (571) 270-1844. The examiner can normally be reached on Monday - Friday 9:00 - 5:30 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Samir Ahmed can be reached at (571) 272-7413 . Customer Service can be reached at (571) 272-2600. The fax number for the organization where this application or proceeding is assigned is (571) 273-7332.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/srk/

/Samir A. Ahmed/
Supervisory Patent Examiner, Art Unit 2624